C. **REMARKS**

Status of the Claims

Claims 1-5, 7-13, 15-21, and 23-27 are currently present in the Application and stand rejected. Claims 1, 11, 19, and 27 are independent claims. In this Response, no claims have been amended, canceled, or added.

Claim Rejections - Alleged Obviousness Under 35 U.S.C. § 103

The Office Action rejects Applicants independent method claims 1 and 27 and dependent claim 5 under 35 U.S.C. § 103 as allegedly being obvious, and therefore unpatentable, over U.S. Patent No. 5,241,594 to Kung (hereinafter "Kung") in view of U.S. Patent No. 6,539,479 to Wu (hereinafter "Wu"). The Office Action rejects Applicants other independent claims, 11 and 19, and dependent claims 12, 17, 20, and 24 as being obvious, and therefore unpatentable, over Kung in view of Wu in further view of U.S. Patent No. 6,668,321 to Nendell et al. (hereinafter "Nendell"). Applicants respectfully traverse the rejections.

Kung teaches a method of logging onto a remote "secure" computer from another "secure" workstation. Importantly, Kung does not teach or suggest sending passwords and data in anyway similar to that claimed by Applicants. Each of Applicants independent claims are directed to securely transmitting data in a network with limitations that include:

- sending a request from a first computer to a second computer prior to establishing a secure connection, the first computer and the second computer included in a plurality of computers;

- receiving a response from the second computer, whereby the response informs the first computer that the second computer accepts encrypted data;
- establishing the secure connection between the first computer and the second computer;
- transmitting a password across the secure connection, the password used to encrypt and decipher the data;
- encrypting the data using the password; and
- transmitting the encrypted data over a non-secure connection.

Contrary to Applicants' claimed limitations, Kung teaches that a user logs onto a first workstation (secure workstation 11) using a user ID and password. The workstation encrypts the password supplied and compares the user ID and encrypted password with a stored encrypted password (stored in database 19a which is stored on workstation 11). If the encrypted password matches, the user is allowed access to secured workstation 11 (see Figure 4, and Kung's description at col. 5, line 37 to col. 6, line 2 and col. 6, lines 23-40). Kung further teaches that the user, once logged onto the secure workstation, can log onto a remote computer (remote computer 13). A secure communication path is established between the secure workstation and the remote computer and the user provides the remote computer with another user ID and another password. The remote computer uses a one-way encryption algorithm, substantially similar to that used by workstation 11, to encrypt the password and compare the supplied user ID and encrypted password to user IDs and encrypted passwords stored on the remote computer (in database 19b, see Figure 4, col. 5, line 37

- col. 6, line 50). Importantly, the password sent over Kung's secure path is not "used to encrypt and decipher … data," as claimed by Applicants. Instead, the password taught by Kung that is transmitted on a secure path is only used to log the user onto the remote computer. Kung never teaches or suggests using the password to encrypt or decipher data. Kung also fails to teach or suggest other limitations claimed in Applicants' independent claims. These shortcomings are detailed below.

First, Kung never teaches or suggests "sending a request from a first computer to a second computer prior to establishing a secure connection, the first computer and the second computer included in a plurality of computers." Instead, Kung teaches that the secure workstation and the remote computer are in a distributed network where the computers are known to one another and that the network interconnecting the computers "incorporates a secure communication path 20a as part of the network 20 that connects a secure user workstation 11 to the remote host computer 13." Nowhere does Kung teach or suggest that the either computer sends a request to the other "prior to establishing a secure connection," as claimed by Applicants.

Next, Kung never teaches or suggests "receiving a response from the second computer, whereby the response informs the first computer that the second computer accepts encrypted data," as claimed by Applicants. Instead, Kung's system relies on each system using a particular one-way encryption algorithm to encrypt the passwords and also teaches that each computer is a "secured" computer that is interconnected to each other using a pre-established "secure communication path 20a." Kung never teaches or suggests one of the computers sending a message back to the other computer indicating that the computer accepts encrypted data.

Next, Applicants claim "establishing the secure connection between the first computer and the second computer." However, as explained above, the computers in Kung's network are always connected by a secure connection, and therefore, while Kung's computers ***use*** a secure connection supplied by the existing infrastructure (network 20), Kung does not teach or suggest ***establishing*** the secure connection between the two computers.

Next, Applicants claim "transmitting a password across the secure connection, the password used to encrypt and decipher the data." As described above, Kung does teach transmitting a user ID and password from the workstation to the remote computer so that a user of the workstation can log onto the remote computer. However, Kung never teaches or suggests using the password "to encrypt and decipher" data, as claimed by Applicants. Instead, the password taught by Kung is simply used to authenticate the user on the remote computer system.

In fact, the Office Action admits that Kung does not teach "implementing the password transferred over the secured communication as the encrypt/decrypt keys." The Office Action further admits that Kung does not teach or suggest using the password to encrypt data. The Office Action further admits that Kung does not teach or suggest transmitting data, encrypted using the password, over a non-secure connection. Indeed, Kung instead teaches that the connection between the workstation and the remote computer is always secure and never teaches or suggests sending data over a non-secure network.

As illustrated above, Kung completely fails to teach or suggest **<u>any</u>** of Applicants' claimed limitations. Applicants respectfully submit that the Office Action misapplies the teachings of Kung to Applicants' claimed invention. Even so, the Office Action still admits that Kung fails to teach or suggest "implementing the password transferred over the secured communication as the encrypt/decryption keys." To overcome the serious shortcomings of Kung, the Office Action alleges that Wu teaches these limitations. Again, as described below, Wu also falls far short of teaching or suggesting Applicants' claim limitations.

In each of Applicants' independent claims, Applicants claim certain limitations regarding the use of the password in encrypting/decrypting data. These limitations include:

- transmitting a password across the secure connection, the password used to encrypt and decipher the data;
- encrypting the data using the password; and
- transmitting the encrypted data over a non-secure connection.

The Office Action contends that Wu teaches these limitations. However, a review of Wu reveals that Wu neither teaches nor suggests these limitations. The Office Action cites Wu, col. 5, lines 45-53, and col. 6, lines 1-10 in support of this contention. These sections of Wu are from Wu's "Summary of the Invention," are included below:

> SUMMARY OF THE INVENTION
>
> In summary, the present invention is a system and method for a server computer and a login procedure executed by a client host computer to establish a session key in a manner that is secure against both passive and active security attacks, and which utilizes the user's password so as to enable the server to determine whether or not the user in

> fact knows the password for the username account specified by the user during the login process.
>
> Prior to a login session, the server computer stores a password verification value x_p for each of a plurality of authorized users of the server computer. Each user generates a password verification value x_p by applying a first one-way hashing function to a password p specified by the user to generate a secret value x_s, and then applying a second one-way function to the secret value x_s to generate x_p.
>
> When a client computer attempts to establish a login session between the server computer and client computer, the following steps are performed. The server computer receives a user identifier from the client computer, and retrieves the password verification value stored by the server for the user. The client computer generates a first secret value w_s and then generates a corresponding first public value w_p by applying the second one-way function to the first secret value w_s. The client computer sends the first public value w_p to the server computer.
>
> The server computer generates a second secret value y_s and then generates a corresponding second public value y_p by applying the second one-way function to the second secret value y_s. The server computer sends the second public value y_p to the client computer. The server computer also generates a server session key K1 by applying a first predefined session key generation function to the first public value w_p, the retrieved password verification value x_p, and the second secret value y_s.
>
> The client computer regenerates the user's secret value x_s, and then generates a client session key K2 by applying a second predefined session key generation function to the second public value y_p, the first secret value w_s, and the regenerated secret value x_s.
>
> Then the client and server computers exchange a set of messages so that each can verify that the other computer's session key is equal to its locally generated session key. The login session is established only if the server computer verifies that the server and client session keys match.

Wu describes a login procedure that establishes a "session key" that is used in a public key/private key encryption protocol. Importantly, Wu never teaches or suggests encrypting ***any*** data with a password. Instead, Wu teaches that a one-way hashing algorithm is applied to a password to generate a "password verification value x_p." Wu then teaches using the password verification value along with a "first public [key] value w_p," and a "second secret value y_s," in order to generate a "server key K1" using a "predefined session key generation function." While Wu does not teach or suggest encrypting data using the password, as claimed by Applicants, Wu does not even teach or suggest using the password to generate the server key. Instead, Wu teaches first using a hash function with the password in order to generate a "password verification value" that is one of three inputs to the session key generation function.

In this Response, as well as other Responses, Applicants have thoroughly explained why the references cited in the Office Actions teach or suggest Applicants' claimed invention. Wu never teaches or suggests encrypting ***anything*** with a password. Neither Kung nor Wu, alone or in combination with one another teach or suggest "*transmitting a password across the secure connection, the password used to encrypt and decipher the data; encrypting the data using the password; and transmitting the encrypted data over a non-secure connection,*" as claimed by Applicants in each of Applicants' independent claims.

The remaining dependent claims each depend, directly or indirectly, on an allowable independent claim, as described above. Therefore, each of the remaining dependent claims is allowable for at least the same reasons that the independent claims are allowable.

Conclusion

As a result of the foregoing, it is asserted by Applicants that the remaining claims in the Application are in condition for allowance, and Applicants respectfully request an early allowance of such claims.

Applicants respectfully request that the Examiner contact the Applicants' attorney listed below if the Examiner believes that such a discussion would be helpful in resolving any remaining questions or issues related to this Application.

Respectfully submitted,

By

Joseph T. Van Leeuwen, Reg. No. 44,383
Van Leeuwen & Van Leeuwen
Attorneys for Applicant
Telephone: (512) 301-6738
Facsimile: (512) 301-6742